Sabita J. Soneji (SBN# 224262)
TYCKO & ZAVAREEI LLP
1970 Broadway, Suite 1070
Oakland, CA 94612
(510) 254-6808
ssoneji@tzlegal.com

Counsel for Plaintiffs and Proposed Classes

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
SOUTHERN DIVISION

JOSEPH MASSARO and CRYSTAL TAYLOR-JONES, *individually, and on behalf of all others similarly situated*,

Plaintiffs,

v.

LOANDEPOT, INC.,

Defendant.

Case No. 8:24-cv-253

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Joseph Massaro and Crystal Taylor-Jones, individually, and on behalf of all others similarly situated, bring this Class Action Complaint ("Complaint") against Defendant loanDepot, Inc. (the "Defendant" or "LDI") for (i) negligence, (ii) invasion of privacy and (iii) unjust enrichment, (iv) violations of the California Unfair Competition Law, (v) violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, and (vi) declaratory judgment and injunctive relief. Plaintiffs make the following allegations on information and belief, except as

to their own actions, which are made on personal knowledge, the investigation of counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This lawsuit is a class action seeking compensation and both declaratory and injunctive relief for Plaintiffs and other LDI customers.

2. LDI, a publicly traded company listed on the New York Stock Exchange under the symbol "LDI," is headquartered in Irvine, California. It boasts a workforce of over 6,000 employees and manages loans valued at more than $140 billion.[1]

3. As more specifically described below, this Complaint concerns a recent targeted ransomware attack and data breach (the "Data Breach") on LDI's network that resulted in unauthorized access to the highly sensitive data of roughly 16.6 million individuals.[2]

4. Due to the Data Breach, members of the class experienced identifiable losses, including the diminished value of their agreement, expenses incurred directly, time spent addressing or reducing the impact of the breach, emotional distress, and the ongoing threat of imminent harm from the exposure of their sensitive personal data.

[1] https://www.loandepot.com/about (last accessed February 6, 2024).
[2] https://media.loandepot.com/news-releases/press-release-details/2024/loanDepot-Provides-Update-on-Cyber-Incident/default.aspx (last accessed February 6, 2024).

5. Upon information and belief, the data compromised in the Data Breach includes, among other things, personally identifiable information ("PII") such as full names, dates of birth, residential addresses, financial details, and social security numbers.

6. Upon information and belief, up to and through January 2024, Defendant obtained the PII of Plaintiffs and Class Members and stored that PII, unencrypted, in an Internet-accessible environment on Defendant LDI's network, from which unauthorized actors used an extraction tool to retrieve sensitive PII belonging to Plaintiffs and Class Members.

7. Plaintiffs' and Class Members' PII, entrusted to the Defendant, its officials, and agents, was compromised and unlawfully accessed as a result of the Data Breach.

8. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Plaintiffs' and Class Members' PII that Defendant collected and maintained, and for Defendant's failure to provide timely and adequate notice to Plaintiffs and other Class Members that their PII had been subject to the unauthorized access of an unknown, unauthorized party.

9. Defendant LDI maintained the PII in a negligent and/or reckless manner. In particular, the PII was maintained on Defendant's network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the

cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' PII was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

10. Further, upon information and belief, Defendant and its employees failed to properly monitor the computer network, IT systems, and integrated service that housed Plaintiffs' and Class Members' PII.

11. LDI's negligence in protecting its clients' PII is especially egregious, especially considering that the Defendant experienced a previous data breach in August 2022, which it only informed its customers about almost a year later in May 2023.

12. As a result of the Defendant's negligent actions, Plaintiffs' and Class Members' identities are now in jeopardy, as the PII collected and stored by the Defendant is now in the possession of malicious cybercriminals. The threats to Plaintiffs and Class Members will persist for the duration of their lifetimes.

13. LDI failed to offer prompt, precise, and sufficient notification to Plaintiffs and Class Members regarding PII lost by the Defendant. Further, Defendant failed to notify its customers of the exact nature of unencrypted information in the possession of unidentified third parties, was unreasonably postponed due to the Defendant's failure to promptly alert affected individuals upon discovering the Data Breach.

14. As a putative remediation for allowing Plaintiffs' and Class Members' PII to be acquired by an unauthorized third-party, Defendant stated that "[t]he Company will notify [the affected] individuals and offer credit monitoring and identity protection services and no cost to them."[3] To date, Defendant has not contacted or offered any actual remediation to the victims of this Data Breach, but this assurance serves as tacit acknowledgement of the significant harm and elevated risk that 16.6 million individuals now face as a result of Defendant's acts and omissions.

15. Indeed, armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to target other phishing and hacking intrusions using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

16. Due to the Data Breach, Plaintiffs and Class Members face an immediate and increased risk of fraud and identity theft. They are now compelled to

[3] *Id.*

diligently monitor their financial accounts to protect against identity theft indefinitely.

17. Plaintiffs and Class Members may also incur out of pocket costs for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

18. By this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was exposed during the Data Breach.

PARTIES

19. Plaintiff Joseph Massaro is a resident and citizen of Palm Springs, California where he intends to remain. He is a Data Breach victim, having applied for mortgage loan refinancing from Defendant in or about June 2021.

20. Plaintiff Crystal Taylor-Jones is a resident and citizen of Calumet City, Illinois where she intends to remain. She is a Data Breach victim, having applied for a mortgage loan from Defendant in or about August 2023.

21. Defendant loanDepot, Inc., is a provider of mortgages and lending services with its headquarters at 6561 Irvine Center Drive, Irvine, California 92610.

22. loanDepot, Inc. is an affiliate or parent company of numerous other companies, including but not limited to: LD Holdings Group LLC, loanDepot.com, LLC, LD Settlement Services, LLC, American Coast Title Company, Inc., melloInsurance Services, LLC, Closing USA of Alabama, LLC, Closing USA LLC,

Closing USA of Arkansas, LLC, Commercial Agency USA, LLC, Closing USA of Delaware, LLC, Closing USA of Utah, LLC, mello Holdings, LLC, mello Home Services, LLC, mello Home, Inc., MTH Mortgage, LLC, MSC Mortgage, LLC, Tri Pointe Connect, LLC, Day One Mortgage, LLC, loanDepot-FB Mortgage, LLC (d/b/a Farm Bureau Mortgage), Heartwood Mortgage, LLC, BRP Home Mortgage, LLC, Henlopen Mortgage, LLC, LGI Mortgage Solutions, LLC, NHC Mortgage, LLC.

23. Defendant loanDepot, Inc. is a corporation formed in Delaware and registered in good standing in California.[4]

JURISDICTION AND VENUE

24. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because at least one member of the putative Class, including one of the Plaintiffs, are citizens of a different state than Defendant, there are roughly 16.6 million putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

25. This Court has personal jurisdiction over Defendant because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conducts substantial business in California and in this District through its

[4] According to the California Secretary of State, LDI's California Registered Corporate Agents are Jackson Yang, Gabriela Gonzalez, Jeffrey Kurtz, Jennifer McLaughlin, Jaclyn Wright, Adam Saldana, Mackenzie Hibler, Alvine Sayre, Jessice Wittry, Angela Castillo, Ashley Sims, and Emily Rendon.

headquarters, offices, parents, and affiliates.

26. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal places of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL BACKGROUND

A. LDI's Business

27. LDI ranks as the fifth largest retail mortgage lender in the United States and holds the position of the second largest nonbank retail originator. Established in 2010, the Defendant has facilitated lending exceeding $275 billion. Presently, LDI employs over 6,000 individuals and serves upwards of 27,000 customers on a monthly basis.[5]

28. On information and belief, LDI maintains the PII of customers, including but not limited to:

a. name, residential address, phone number and email address

b. date of birth

c. demographic information

d. Social Security number

e. tax identification number

[5] *See supra*, n.1.

f. financial information

g. medication information

h. health insurance information

i. photo identification

j. employment information, and

k. other information that Defendant may deem necessary to provide its services.

29. Plaintiffs and Class Members directly or indirectly entrusted Defendant with sensitive and confidential PII, which includes information that is static, does not change, and can be used to commit myriad financial and other crimes.

30. Due to the profoundly sensitive and personal nature of the information obtained, stored, and accessible to the defendant, the Defendant pledged to, among other commitments: Maintain the confidentiality of PII; adhere to industry standards concerning data security and PII; educate individuals about their legal obligations and adhere to all federal and state laws safeguarding PII; exclusively utilize and disclose PII for purposes related to medical care and treatment; and promptly notify affected individuals if their PII is divulged without authorization.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from unauthorized disclosure.

32. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

33. Plaintiffs and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their PII confidential and securely maintained, to use such PII solely for business purposes, and to prevent the unauthorized disclosures of the PII.

34. If Plaintiffs and Class Members had known that Defendant would not take reasonable and appropriate steps to protect their sensitive and valuable PII, they would not have entrusted it to Defendant.

B. LDI Fails to Safeguard Customer PII

35. On or around January 8, 2024, Defendant LDI posted the following online:

> LoanDepot is experiencing a cyber incident. We have taken certain systems offline and are working diligently to restore normal business operations as quickly as possible. We are working quickly to understand the extent of the incident and taking steps to minimize its impact. The Company has retained leading forensics experts to aid in our investigation and is working with law enforcement. We sincerely apologize for any impacts to our customers, and we are focused on resolving these matters as soon as possible.[6]

36. Over the next several days and weeks, Defendant continued to

[6] https://loandepot.cyberincidentupdate.com/ (last accessed February 3, 2024)

intermittently post updates to its website alerting customers when its various subsidiaries' payment portals were reactivated.[7] On or about January 22, 2024, Defendant posted the following statement in response to the Data Breach:

> The Company has been working diligently with outside forensics and security experts to investigate the incident and restore normal operations as quickly as possible. The Company has made significant progress in restoring our loan origination and loan servicing systems, including our MyLoanDepot and Servicing customer portals.
>
> Although its investigation is ongoing, the Company has determined that an unauthorized third party gained access to sensitive personal information of approximately 16.6 million individuals in its systems. The Company will notify these individuals and offer credit monitoring and identity protection services at no cost to them.
>
> "Unfortunately, we live in a world where these types of attacks are increasingly frequent and sophisticated, and our industry has not been spared. We sincerely regret any impact to our customers," said LoanDepot CEO Frank Martell. "The entire LoanDepot team has worked tirelessly throughout this incident to support our customers, our partners and each other. I am pleased by our progress in quickly bringing our systems back online and restoring normal business operations."
>
> "Our customers are at the center of everything we do," said Jeff Walsh, President of LDI Mortgage. "I'm really proud of our team, and we're glad to be back to doing what we do best: enabling our customers across the country to achieve their financial goals and dreams of homeownership."
>
> The Company is committed to keeping its customers, partners and employees informed and will provide any additional operational updates on our microsite at loandepot.cyberincidentupdate.com.[8]

[7] *Id.*

[8] https://media.loandepot.com/news-releases/press-release-details/2024/loanDepot-Provides-Update-on-Cyber-Incident/default.aspx (last accessed February 3, 2024).

37. To date, LDI's investigation has determined that the private information of roughly 16.6 million customers and other affiliated individuals was accessed and compromised by an unauthorized user on or about January 8, 2024.

38. It is likely the Data Breach was targeted at Defendant due to its status as a financial services provider that collects, creates, and maintains sensitive PII.

39. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data of specific individuals, including (among other things) the PII of Plaintiffs and the Class Members.

40. While Defendant LDI stated in its public notice it would directly notify the affected individuals and that it is committed to keeping the victims informed, upon information and belief Defendant has not yet directly notified Plaintiffs or Class Members.

41. Upon information and belief, and based on the type of cyberattack, it is plausible and likely that Plaintiffs' PII was stolen in the Data Breach. Plaintiffs further believe their PII was likely subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals.

42. Defendant had a duty to adopt appropriate measures to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties.

43. In response to the Data Breach, Defendant LDI admits it worked with external "security experts" to determine the nature and scope of the incident and purports to have taken steps to secure the systems. Defendant LDI admits additional

security was required, but there is no indication whether these steps will be adequate to protect Plaintiffs' and Class Members' PII going forward.

44. Because of the Data Breach, data thieves were able to gain access to Defendant's private systems on January 8, 2024, and were able to compromise, access, and acquire the protected PII of Plaintiffs and Class Members.

45. LDI had obligations created by contract, industry standards, common law, and its own promises and representations made to Plaintiffs and Class Members to keep their PII confidential and to protect them from unauthorized access and disclosure.

46. Plaintiffs and the Class Members reasonably relied (directly or indirectly) on Defendant's sophistication to keep their sensitive PII confidential; to maintain proper system security; to use this information for business purposes only; and to make only authorized disclosures of their PII.

47. Plaintiffs' and Class Members' unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions, and due to the utter failure to protect Class Members' PII. Criminal hackers obtained their PII because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The heightened risks to Plaintiffs and Class Members will remain for their respective lifetimes.

C. Data Breach was a Foreseeable Risk and Defendant Knew or Should Have Known That LDI Was a Target of Cybercriminals

48. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the mortgage industry and other industries holding significant amounts of PII preceding the date of the breach.

49. In light of recent high profile data breaches at other financial services companies, Defendant knew or should have known that their electronic records and PII they maintained would be targeted by cybercriminals and ransomware attack groups.

50. Defendant LDI knew or should have known that these attacks were common and foreseeable.

51. Indeed, LDI itself was subject to a separate data breach in August 2022, which LDI waited nearly a year (until May 2023) to disclose to its customers,

52. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[9]

53. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad

[9] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/ (last accessed Oct. 11, 2023).

(268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals

54. Consequently, the rise in such attacks, along with the associated risk of future occurrences, was well-known to both the general public and to anyone within Defendant's industry, including Defendant themselves.

55. Recognizing these substantial risks, LDI makes its "Privacy Policy" available to customers and potential customers on its website. Within that policy, and as an incentive for customers to provide PII and other confidential information, LDI has made specific representations and assurances, including the following:

> "**Safeguarding Personally Identifiable Information**
>
> - We have adopted policies and procedures designed to protect your personally identifiable information from unauthorized use or disclosure.
>
> - We have implemented physical, electronic, and procedural safeguards to maintain confidentiality and integrity of the personal information in our possession and to guard against unauthorized access. These include among other things, procedures for controlling access to your files, building security programs and information technology security measures such as the use of passwords, firewalls, virus prevention and use detection software.
>
> - We continue to assess new technology as it becomes available and to upgrade our physical and electronic security systems as appropriate.

> **loanDepot Security Policy**
>
> loanDepot takes steps to safeguard your personal and sensitive information through industry standard physical, electronic, and operational policies and practices. All data that is considered highly confidential data can only be read or written through defined service access points, the use of which is password-protected. The physical security of the data is achieved through a combination of network firewalls and servers with tested operating systems, all housed in a secure facility. Access to the system, both physical and electronic, is controlled and sanctioned by a high-ranking manager.
>
> Sharing Information with Companies That Provide Services for Us:
>
> We share personally identifiable information about you, as required or permitted by law, with third parties, such as service providers who assist us in the in the administration, processing, closing, settlement, title or other insuring, servicing, and sale of your loan, or other service providers who assist us in fulfilling products and services for you. These third parties include among others, loan origination system providers, lenders, title companies, appraisers, insurance companies, real estate companies, underwriting services, notary services, processing services, printing companies, document providers, software and technology providers, fraud detection companies, marketing services providers, and purchasers of loans. Our policy is to require third party service providers to enter into confidentiality agreements with us, prohibiting them from using any personally identifiable information they obtain for any other purpose other than those for which they were retained or as required by law."

56. Given the acknowledged risks, LDI neglected to take action to establish reasonable and easily accessible data security protocols and practices to prevent the exposure of its customers' highly sensitive information. This disregard and violation of its commitments and legal duties to customers and state regulations is evident.

D. LDI Failed to Comply with FTC Guidelines

57. The Federal Trade Commission ("FTC") has issued several guides for businesses, emphasizing the significance of adopting reasonable data security measures. As per the FTC, integrating data security considerations into all business decisions is imperative.

58. In 2016, the FTC revised its document, "Protecting Personal Information: A Guide for Business," setting forth cybersecurity directives for businesses. These guidelines emphasize the necessity for businesses to safeguard personal customer information, securely dispose of unnecessary data, encrypt information stored on computer networks, comprehend their network's vulnerabilities, and institute policies to address any security issues promptly.[10] Additionally, the guidelines advise businesses to utilize an intrusion detection system to promptly detect breaches, monitor all incoming traffic for signs of attempted hacking, scrutinize for substantial data transmissions from the system, and have a prepared response plan in case of a breach.[11]

59. Additionally, the FTC advises companies against retaining PII longer than necessary for transaction authorization purposes, restricting access to sensitive

[10] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed February 3, 2024).

[11] *Id.*

data, mandating the use of complex passwords for network access, employing industry-proven security methods, monitoring the network for any suspicious activity, and ensuring that third-party service providers have implemented adequate security measures.

60. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

61. These FTC enforcement actions include actions against mortgage lenders and partners like the Defendant.

62. Defendant failed to properly implement appropriate data security practices.

63. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers and other impacted individuals' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C.§ 45.

64. Throughout, the Defendant was entirely cognizant of their responsibility to safeguard the PII it collects and keeps. They were also well aware

of the substantial consequences that would ensue from their failure to fulfill this obligation.

65. The Defendant's failure to enact reasonable and appropriate data security measures directly contradicted the assurances provided to its customers in its Privacy Policy, thus constituting significant misrepresentations.

E. LDI Failed to Comply with Industry Standards

66. As demonstrated above, experts in cybersecurity consistently pinpoint mortgage lenders and their partners as especially susceptible to cyberattacks due to the inherent value of the PII they gather and retain.

67. Numerous best practices have been identified, which mortgage lenders like the Defendant should, at the very least, adopt. These include but are not limited to: educating all employees; using strong passwords; employing multi-layer security, such as firewalls, anti-virus, and anti-malware software; encrypting data to render it unreadable without a key; implementing multi-factor authentication; backing up data; and restricting access to sensitive data to only authorized employees.

68. Additional cybersecurity best practices that are considered standard in the mortgage industry involve installing suitable malware detection software; monitoring and restricting network ports; safeguarding web browsers and email management systems; configuring network systems such as firewalls, switches, and routers; overseeing and securing physical security systems; fortifying against

potential communication system vulnerabilities; and conducting staff training on crucial aspects.

69. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

70. The foregoing frameworks are existing and applicable industry standards in the mortgage industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

F. LDI's Breach

71. Defendant LDI breached its duties to Plaintiffs and Class Members, or acted negligently and recklessly, by failing to adequately maintain and safeguard its data systems and the application flow of its website. Additionally, it intentionally misrepresented to them the measures it would undertake to safeguard their confidential information. Defendant's unlawful behavior encompasses, among other things, the following actions or omissions:

a. Failing to uphold a sufficient data security system to mitigate the likelihood of data breaches and cyber-attacks.

b. Insufficiently safeguarding PII.

c. Inadequately monitoring their own data security systems for potential intrusions.

d. Neglecting to verify that their vendors, who have access to their computer systems and data, implemented reasonable security protocols.

e. Neglecting to guarantee the confidentiality and integrity of electronic PII it generated, received, stored, and/or transmitted.

f. Failing to establish technical policies and procedures for electronic information systems that store electronic PII, restricting access solely to authorized individuals or software programs.

g. Failing to establish policies and procedures to prevent, detect, mitigate, and rectify security breaches.

h. Neglecting to establish protocols for routinely reviewing records of information system activity, including audit logs, access reports, and security incident tracking reports.

i. Failing to guard against foreseeable threats or risks to the security or integrity of electronic PII.

j. Failing to adequately train all members of their workforce on PII-related policies and procedures.

k. Failing to render the electronic PII they maintained inaccessible, unreadable, or indecipherable to unauthorized individuals.

l. Violating Section 5 of the FTC Act by failing to adhere to FTC guidelines for cybersecurity.

m. Neglecting to comply with the cybersecurity industry standards outlined previously, and

n. Otherwise violating their responsibilities to safeguard the PII of Plaintiffs and Class Members.

72. LDI negligently and unlawfully failed to protect the PII of Plaintiffs and Class Members, as cyberthieves were able to gain access to Defendant's online loan application flow, resulting in unauthorized actors obtaining unsecured and unencrypted PII.

73. Consequently, as detailed below, Plaintiffs and Class Members are currently confronted with an elevated risk of fraud and identity theft. Moreover, they have also suffered the loss of the agreed-upon benefits with Defendant.

G. Data Breaches Cause Disruption and Increased Risk of Fraud and Identity Theft

74. Cyberattacks and data breaches targeting mortgage companies such as the Defendant pose particular challenges as they can significantly disrupt the daily lives of individuals affected by the incident.

75. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[12]

76. This is because any individual affected by a data breach faces severe consequences, regardless of the data's nature. Criminals steal PII with the intent to profit from it. They achieve this by selling the acquired data on the black market to identity thieves who aim to exploit and harass victims, assuming their identities to conduct illicit financial transactions. Since a person's identity resembles a puzzle, the more accurate pieces of data an identity thief obtains, the simpler it becomes to impersonate the victim or engage in harassment or surveillance. For instance, armed with just a name and date of birth, a data thief can employ "social engineering," a hacking technique, to acquire more personal information, such as login credentials or a Social Security number. Social engineering involves manipulating individuals using previously obtained information to extract additional confidential or personal data through tactics like spam calls, text messages, or phishing emails.

77. The FTC advises identity theft victims to undertake various measures to safeguard their personal and financial information following a data breach. These

[12] *See* U.S. GOV. ACCOUNTING OFFICE, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (2007) https://www.gao.gov/new.items/d07737.pdf.

steps include reaching out to one of the credit bureaus to initiate a fraud alert (considering an extended fraud alert lasting 7 years if one's identity is stolen), reviewing credit reports, contacting companies to dispute fraudulent charges, implementing a credit freeze, and rectifying any errors on their credit reports.[13]

78. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

79. Identity thieves may exploit Social Security numbers in various ways, such as acquiring a driver's license or official identification card under the victim's name with the thief's photograph, claiming government benefits using the victim's name and Social Security number, or filing a fraudulent tax return using the victim's information. Further, they might use the victim's Social Security number to secure employment, lease a residence, or access medical services in the victim's name. In some cases, they may even provide the victim's personal information to law enforcement during an arrest, resulting in the issuance of an arrest warrant in the victim's name.

80. Moreover, theft of PII is also gravely serious because PII is an extremely valuable property right.[14]

---

[13] *See IdentityTheft.gov*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Steps (last accessed February 6, 2024).

[14] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*,

81. The value of PII is self-evident, especially considering the significance of "big data" in corporate America and the potential severe consequences of cyber theft, which can include lengthy prison sentences. Even a straightforward risk-reward analysis underscores the substantial market value of PII.

82. It is important to acknowledge that there could be a significant time gap, spanning years, between the occurrence of harm and its discovery, as well as between the theft of PII and its subsequent use.

83. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[15]

84. PII is such a valuable commodity to identity-thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

---

15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[15] GAO Report, at p. 21.

85. Accordingly, there is a high likelihood that entire sets of stolen information have either been or are yet to be sold on the black market, indicating that Plaintiffs and Class Members face an elevated risk of fraud and identity theft for many years to come.

86. Consequently, Plaintiffs and Class Members are required to vigilantly monitor their financial and medical accounts for many years to come.

87. PII can sell for as much as $363 per record according to the Infosec Institute.[16] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for many years.

88. For instance, the Social Security Administration has cautioned that identity thieves can utilize an individual's Social Security number to request additional credit lines. Such fraudulent activities might remain unnoticed until debt collection calls begin months or even years later. Furthermore, stolen Social Security numbers enable thieves to file fraudulent tax returns, claim unemployment benefits, or seek employment under false identities. Detecting each of these fraudulent activities poses significant challenges. For example, individuals may remain unaware that their Social Security number was used to apply for unemployment

[16] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

benefits until law enforcement informs their employer of the suspected fraud. Typically, fraudulent tax returns are only detected when an individual's genuine tax return is rejected.

89. Moreover, it is not an easy task to change or cancel a stolen Social Security number:

> An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[17]

90. As anticipated, this data commands a significantly higher price on the black market. Martin Walter, senior director at the cybersecurity firm RedSeal, elaborated, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[18]

91. Because of the value of its collected and stored data, the mortgage industry has experienced disproportionally higher numbers of data theft events than

[17] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[18] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, COMPUTER WORLD (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

other industries.

92. Hence, the Defendant was aware or should have been aware of these threats and should have bolstered its data and email management systems accordingly. The Defendant was made aware of the significant and foreseeable risk of harm resulting from a data breach yet failed to adequately prepare for this risk.

93. As detailed above, identity thieves can and do use pieces of PII obtained in data breaches to take on the victim's identity, or otherwise harass or track the victim. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

94. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[19]

[19] "Fullz" is a term used by fraudsters to refer to comprehensive data containing the victim's information, including but not limited to their name, address, credit card details, social security number, date of birth, and more. Generally, the more data obtained about a victim, the greater the potential profit from exploiting those credentials. Fullz typically fetch higher prices compared to standard credit card information, often selling for up to $100 per record or more on the dark web. These Fullz can be monetized in various ways, such as conducting bank transactions over the phone using the acquired authentication details. Even "dead Fullz," which are Fullz associated with expired credit cards, can still serve multiple illicit purposes, including tax refund fraud, ordering credit cards in the victim's name, or establishing a "mule account" (an account that receives fraudulent money transfers from compromised accounts) without the victim's awareness. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm,* Krebs on Security (Sep. 18, 2014),

95. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

96. The emergence of "Fullz" packages indicates that the pilfered PII from the Data Breach can readily be linked and associated with Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In essence, even if certain details like emails, phone numbers, or credit card numbers were not originally part of the exfiltrated PII from the Data Breach, criminals can still effortlessly compile a Fullz package and repeatedly sell it at inflated prices to dishonest operators and criminals, such as illicit telemarketers and scammers.

97. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members.

98. Hence, even if specific details (like insurance information) were not compromised in the data breach, criminals can still readily compile a comprehensive "Fullz" package. This exhaustive dossier can then be sold—and subsequently resold indefinitely—to deceitful operators and other criminals, such as illicit telemarketers

https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/.

and scammers.

H. Data Breaches Are Preventable

99. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[20]

100. To prevent and detect cyber-attacks and/or ransomware attacks, the Defendant could and should have implemented the following measures, as advised by the United States Government:

- Establish an awareness and training initiative. Given that end users are often targeted, it's essential for employees and individuals to understand the ransomware threat and how it is typically disseminated.
- Activate robust spam filters to obstruct phishing emails from reaching end users and employ authentication mechanisms such as Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to thwart email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Configure anti-virus and anti-malware software to perform

[20] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

automated regular scans.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have written access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Deploy Software Restriction Policies (SRP) or alternative controls to block the execution of programs from typical ransomware locations, like temporary folders associated with popular Internet browsers or compression/decompression utilities, such as the AppData/LocalAppData folder.

- Evaluate the option of deactivating Remote Desktop Protocol (RDP) if it's not currently in use.

- Employ application whitelisting, which permits systems to run only programs that are recognized and authorized by the security policy.

- Run operating system environments or specific programs within a virtualized environment.

- Classify data according to organizational significance and establish both physical and logical segregation of networks and data for distinct organizational units.[21]

101. To prevent and detect cyber-attacks or ransomware attacks, Defendant

[21] *Id.,* at 3-4.

could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

A. Secure Internet-Facing Assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

B. Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

C. Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

D. Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

E. Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

F. Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[22]

102. Given that Defendant was storing the sensitive PII of its current and former customers and applicants, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

I. Plaintiffs' and Class Members' Damages

103. To date, Defendant has done nothing to provide Plaintiffs and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

104. Plaintiffs and Class Members have been damaged by the compromise of their PII in the Data Breach.

105. Plaintiffs and Class Members' full names, addresses, tax identification numbers, and Social Security numbers were compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's software.

[22] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

106. Since being notified of the Data Breach, Plaintiffs has spent time dealing with the impact of the Data Breach, valuable time Plaintiffs otherwise would have spent on other activities, including but not limited to work and/or recreation.

107. Due to the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring their accounts for fraudulent activity.

108. Plaintiffs' PII was compromised as a direct and proximate result of the Data Breach.

109. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

110. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach.

111. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

112. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as

potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

113. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

114. Plaintiffs and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

115. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiffs and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's systems and Plaintiffs' and Class Members' PII. Thus, Plaintiffs and Class Members did not get what they paid for and agreed to.

116. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and sensitive information for misuse.

117. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred

to remedy or mitigate the effects of the Data Breach relating to:

a. reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. purchasing credit monitoring and identity theft prevention;

c. placing "freezes" and "alerts" with reporting agencies;

d. spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. contacting financial institutions and closing or modifying financial accounts; and

f. closely reviewing and monitoring Social Security numbers, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

118. Further, Plaintiffs and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of adequate security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing PII is not accessible online and that access to such data is password protected.

119. As a result of Defendant's conduct, Plaintiffs and Class Members are

forced to live with the anxiety that their PII may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

120. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

J. Plaintiffs' Experiences

1. Plaintiff Massaro

121. Plaintiff Massaro is a current customer of the Defendant and has been since June 2021.

122. Plaintiff Massaro applied for and received mortgage loan refinancing from Defendant in or about June 2021.

123. As a condition for and/or receiving Defendant's home refinancing services, Plaintiff Massaro was required to provide his sensitive private information, including, *inter alia*, his name, date of birth, residential address, financial information, and social security number.

124. Plaintiff Massaro is very careful about sharing his sensitive PII. Plaintiff Massaro has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

125. If Plaintiff Massaro knew that Defendant would not take reasonable and appropriate steps to protect his sensistive PII, he would never have entrusted it to

them.

126. Plaintiff Massaro first learned of the Data Breach after seeing a post about the Breach on social media on or about January 26, 2024. Plaintiff Massaro believes he is part of the Data Breach based on the scope of the Data Breach and the fact that he provided his Private Information to the Defendant.

127. Based on the information he provided to Defendant, Plaintiff Massaro has reason to believe that his PII including, but not limited to, his name, address, phone number, email address, Social Security number, and financial information were compromised in this Data Breach.

128. As a result of the Data Breach, Plaintiff Massaro made reasonable efforts to mitigate the impact of the Data Breach after receiving notice of the Data Breach, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud.

129. Plaintiff Massaro has spent significant time and will continue to spend valuable hours for the remainder of his life, that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

130. Plaintiff Massaro suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant maintained belonging to Plaintiff Massaro; (b) violation of his privacy rights; (c) the

theft of his PII; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

131. As a result of the Data Breach, Plaintiff Massaro has also suffered emotional distress as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Massaro is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

132. As a result of the Data Breach, Plaintiff Massaro anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of his life.

2. Plaintiff Taylor-Jones

133. Plaintiff Taylor-Jones is a current customer of the Defendant and has been since in or about August 2023.

134. Plaintiff Taylor-Jones applied for and received a mortgage loan from Defendant in or about August 2023.

135. As a condition for and/or receiving Defendant's mortgage loan services, Plaintiff Taylor-Jones was required to provide her sensitive private information,

including, *inter alia*, her name, date of birth, residential address, financial information, and social security number.

136. Plaintiff Taylor-Jones is very careful about sharing her sensitive PII. Plaintiff Taylor-Jones has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

137. If Plaintiff Massaro knew that Defendant would not take reasonable and appropriate steps to protect his sensitive PII, he would never have entrusted it to them.

138. Plaintiff Taylor-Jones first learned of the Data Breach after seeing a post about the Breach on social media on or about January 26, 2024. Plaintiff Taylor-Jones believes she is part of the Data Breach based on the scope of the Data Breach and the fact that he provided his Private Information to the Defendant.

139. Based on the information she provided to Defendant, Plaintiff Taylor-Jones has reason to believe that her PII including, but not limited to, her name, address, phone number, email address, Social Security number, and financial information were compromised in this Data Breach.

140. As a result of the Data Breach, Plaintiff Taylor-Jones made reasonable efforts to mitigate the impact of the Data Breach after receiving notice of the Data Breach, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud.

141. Plaintiff Taylor-Jones has spent significant time and will continue to spend valuable hours for the remainder of her life, that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

142. Plaintiff Taylor-Jones suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant maintained belonging to Plaintiff Taylor-Jones; (b) violation of her privacy rights; (c) the theft of her PII; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

143. As a result of the Data Breach, Plaintiff Taylor-Jones has also suffered emotional distress as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Taylor-Jones is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

144. As a result of the Data Breach, Plaintiff Taylor-Jones anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of her life.

CLASS ACTION ALLEGATIONS

145. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated.

146. Plaintiffs propose the following Class and Subclass definitions, subject to amendment as appropriate:

Nationwide Class

All persons within the United States whom the Defendant has identified as being affected by the Data Breach, including those who received a notification regarding the Data Breach (the "Class").

Illinois Subclass

Persons located in the state of Illinois whom the Defendant has identified as being affected by the Data Breach, including those who received a notification regarding the Data Breach (the "Illinois Subclass").

147. Excluded from the Classes are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Further excluded from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

148. Plaintiffs reserve the right to amend or modify the Class and/or Illinois

Subclass definitions as this case progresses.

149. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of thousands of individuals whose sensitive data was compromised in the Data Breach.

150. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. if Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII;

b. if Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

c. if Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

d. if Defendant owed a duty to Class Members to safeguard their PII;

e. if Defendant breached their duty to Class Members to safeguard their PII;

f. if Defendant knew or should have known that their data security systems and monitoring processes were deficient;

g. if Defendant should have discovered the Data Breach sooner;

h. if Plaintiffs and Class Members suffered legally cognizable damages

as a result of Defendant's misconduct;

i. if Defendant's conduct was negligent;

j. if Defendant's breach implied contracts with Plaintiffs and Class Members;

k. if Defendant were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

l. if Defendant failed to provide notice of the Data Breach in a timely manner, and;

m. if Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

151. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

152. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

153. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these

common issues in a single action has important and desirable advantages of judicial economy.

154. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

155. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

156. Likewise, particular issues under Rule 42(d)(l) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. if Defendant failed to timely notify the public of the Data Breach;

b. if Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. if Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. if Defendant's failure to institute adequate protective security measures amounted to negligence;

e. if Defendant failed to take commercially reasonable steps to safeguard consumer PII; and

f. if adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

157. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant LDI.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Class)

158. Plaintiffs re-allege and incorporate by reference herein all allegations contained in the foregoing paragraphs.

159. Plaintiffs and the Class entrusted Defendant with their PII on the

premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

160. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed.

161. By collecting and storing this data in their computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard their computer system—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

162. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

163. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and individuals who entrusted them with PII, which is recognized by laws and regulations, as well as

common law. Defendant was in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

164. Defendant's duty to use reasonable security measures required Defendant to reasonably protect confidential data from any intentional or unintentional use or disclosure.

165. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

166. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant are bound by industry standards to protect confidential PII.

167. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. failing to adequately monitor the security of their networks and systems;

d. failing to have in place mitigation policies and procedures;

e. allowing unauthorized access to Class Members' PII;

f. failing to detect in a timely manner that Class Members' PII had been compromised; and

g. failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

168. Defendant owed to Plaintiffs and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the data breach. This duty is required and necessary for Plaintiffs and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the data breach.

169. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

170. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security

practices to safeguard Plaintiffs' and Class Members' PII.

171. Defendant owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiffs' and Class Members' PII.

172. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

173. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiffs and Class Members and the importance of exercising reasonable care in handling it.

174. Defendant breached its duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiffs and Class Members—which actually and proximately caused the Data Breach and injured Plaintiffs and Class Members.

175. Defendant further breached its duties by failing to provide reasonably timely notice of the data breach to Plaintiffs and Class Members, which actually and proximately caused and exacerbated the harm from the data breach and Plaintiffs and Class Members' injuries-in-fact. As a direct and traceable result of Defendant's

negligence and/or negligent supervision, Plaintiffs and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

176. Defendant's breach of its common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiffs and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the data breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Invasion of Privacy
(On behalf of the Plaintiffs and the Class)

177. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in the foregoing paragraphs.

178. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

179. Defendant owed a duty to Plaintiffs and Class Member to keep their PII confidential.

180. The unauthorized disclosure and/or acquisition (*i.e.,* theft) by a third

party of Plaintiffs' and Class Members' PII is highly offensive to a reasonable person.

181. Defendant's reckless and negligent failure to protect Plaintiffs' and Class Members' PII constitutes an intentional interference with Plaintiffs' and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

182. Defendant's failure to protect Plaintiffs' and Class Members' PII acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

183. Defendant knowingly did not notify Plaintiffs and Class Members in a timely fashion about the Data Breach.

184. Because Defendant failed to properly safeguard Plaintiffs' and Class Members' PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

185. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiffs and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

186. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII is still maintained by Defendant with their inadequate cybersecurity system and policies.

187. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiffs and the Class.

188. Plaintiffs, on behalf of themselves and Class Members, seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' PII.

189. Plaintiffs, on behalf of themselves and Class Members, seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

190. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in the foregoing paragraphs.

191. Defendant published its "Privacy Policy" to Plaintiffs and the Class as customers on its website. In that policy, and Defendant promised, as consideration to customers providing private and sensitive PII to take appropriate steps to safeguard personally identifiable information by implementing industry standard physical, electronic, and operational policies and practices.

192. Defendant further represented, and continue to represent as further

consideration that it had implemented physical, electronic, and procedural safeguards to maintain confidentiality and integrity of the personal information in Defendant's possession, to guard against unauthorized access, and that it would continue to assess new technology as it becomes available and to upgrade its physical and electronic security systems as appropriate.

193. These promises by Defendant constituted an implied contract between Defendant and Plaintiffs and Class Members. Defendant breached these implied contracts by failing to provide the promised adequate security to protect the private and sensitive PII from disclosure to third parties. Defendant had notice and knew that its cybersecurity practices were inadequate would cause injury to Plaintiffs and the Class.

194. As a proximate result of Defendant's breach of contract, the private and sensitive PII of Plaintiffs and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

195. Defendant continues to breach and cause injury to Plaintiffs and the Class since their PII is still maintained by Defendant with their inadequate cybersecurity system and policies.

196. Plaintiffs, on behalf of themselves and Class Members, seek actual and consequential compensatory damages for Defendant's breach of contract, which includes the value of the privacy interest disclosed by Defendant, the costs of future

monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

197. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in the foregoing paragraphs.

198. This count is pleaded in the alternative to breach of implied contract above.

199. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and the Class Members.

200. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

201. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its agents and in so doing provided Defendant with their PII. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

202. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiffs and Class Members for business purposes.

203. Plaintiffs and Class Members conferred a monetary benefit on Defendant, by paying Defendant as part of Defendant rendering financial services, a portion of which was to have been used for data security measures to secure Plaintiffs' and Class Members' PII, and by providing Defendant with their valuable PII.

204. Defendant was enriched by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid the data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

205. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

206. Defendant acquired the monetary benefit and PII through inequitable means in that it failed to disclose the inadequate security practices previously

alleged.

207. If Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

208. Plaintiffs and Class Members have no adequate remedy at law.

209. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

210. As a direct and proximate result of Defendant's conduct, Plaintiffs and

Class Members have suffered and will continue to suffer other forms of injury and/or harm.

211. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

FIFTH CAUSE OF ACTION
Violation of the California Unfair Competition Law
[Cal. Bus. & Prof. Code § 17200, *et seq*. – Unlawful Business Practices]
(On Behalf of Plaintiffs and the Class)

212. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in the foregoing paragraphs.

213. LDI violated Cal. Bus. and Prof. Code § 17200, et seq., by engaging in unlawful, unfair, or fraudulent business acts and practices and unfair, deceptive, untrue, or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the Class.

214. LDI engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and Class Members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and

Class Members' PII in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires LDI to take reasonable methods for safeguarding the PII of Plaintiffs and the Class Members.

215. In addition, LDI engaged in unlawful acts and practices by failing to disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

216. As a direct and proximate result of LDI's unlawful practices and acts, Plaintiffs and Class Members were injured and lost money or property, including but not limited to the price received by LDI for the products and services, the loss of Plaintiffs' and Class Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described herein.

217. LDI knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII and that the risk of a data breach or theft was highly likely. LDI's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and Class Members.

218. Plaintiffs, on behalf of the Class, seeks relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiffs and Class Members of money or property that LDI may have acquired by means of its unlawful,

and unfair business practices, disgorgement of all profits accruing to LDI because of its unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

SIXTH CAUSE OF ACTION
Violations of the Illinois Consumer Fraud and Deceptive Business Practices
[Act 815 Ill. Comp. Stat. §§ 505/1, *et seq.*]
(On Behalf of Plaintiff Taylor-Jones and the Illinois Subclass)

219. Plaintiff Taylor-Jones re-alleges and incorporates by reference herein all of the allegations contained in the foregoing paragraphs and brings this claim on behalf of herself and the Illinois Subclass.

220. Plaintiff Taylor-Jones and the Illinois Subclass are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiff, the Class, and Defendant are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

221. Defendant engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendant engages in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

222. Plaintiff Taylor-Jones may bring claims under the ICFA because there is a "consumer nexus" between her and consumers with respect to Defendant's unfair and deceptive trade practices.

223. Taylor-Jones' conduct mirrored that of other consumers, as she reasonably trusted the defendant's public statements and omissions concerning their

data security measures. Specifically, Defendant's statements, including its privacy policy, states Defendant will use reasonable security measures to protect its network from cybercriminals and ransomware attacks.

224. The Defendant's statements and omissions regarding its data security measures, along with its failure to establish and uphold reasonable data security standards, are of concern to all individuals. This is because a reasonable consumer, similar to Plaintiff Taylor-Jones, either does or is likely to depend on these statements when providing their PII.

225. The Defendant's conduct raises consumer protection issues because they assured consumers that they implemented adequate data security measures, when in reality, they did not. Defendant's conduct also involves consumer protection concerns because Defendant's failure to implement and maintain reasonable data security measures enabled the ContiGroup to access and exfiltrate the PII of consumers from its network. In turn, Plaintiff Taylor-Jones' and the Illinois Subclass Members' PII is on the dark web.

226. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the ICFA, including: (i) failing to maintain adequate data security to keep Plaintiff Taylor-Jones and the Illinois Subclass Members' sensitive PII from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards

pertaining to data security, including the FTC Act; (ii) failing to disclose or omitting material facts to Plaintiff and the Class regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the PII of Plaintiff Taylor-Jones and the Illinois Subclass; (iii) failing to disclose or omitting materials facts to Plaintiff Taylor-Jones and the Illinois Subclass about Defendant's failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII of Plaintiff Taylor-Jones and the Illinois Subclass; and (iv) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff's and the Class's PII and other personal information from further unauthorized disclosure, release, data breaches, and theft.

227. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about their inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff Taylor-Jones and the Illinois Subclass and defeat their reasonable expectations about the security of their PII.

228. Defendant intended that Plaintiff Taylor-Jones and the Illinois Subclass rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

229. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that

applied to the Illinois Subclass. Plaintiff Taylor-Jones and the Illinois Subclass have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

230. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiff Taylor-Jones and the Illinois Subclass of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, et seq.

231. As a result of Defendant's wrongful conduct, Plaintiff Taylor-Jones and the Illinois Subclass were injured in that they never would have provided their PII to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII from being hacked and taken and misused by others.

232. As a direct and proximate result of Defendant's violations of the CFA, Plaintiff Taylor-Jones and the Illinois Subclass have suffered harm: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity

theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff Taylor-Jones and Illinois Subclass Members.

233. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff Taylor-Jones and the Illinois Subclass seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the CFA.

234. The relief sought by Plaintiff Taylor-Jones will aid consumers by requiring the Defendant to enhance its data security practices through injunctive relief.

SEVENTH CAUSE OF ACTION
Declaratory Judgment and Injunctive Relief
(On Behalf of Plaintiffs and the Class)

235. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in the foregoing paragraphs.

236. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious, and which

violate the terms of the federal and state statutes described above.

237. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiffs alleges Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiffs and the Class continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

238. Under its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed, and continues to owe, a legal duty to employ reasonable data security to secure the PII it possesses, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

b. Defendant breached, and continues to breach, its duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

c. Defendant's breach of its legal duty continues to cause harm to Plaintiffs and the Class.

239. If an injunction is not granted, Plaintiffs and the Class will face irreparable harm and lack an effective legal recourse in the event of another breach

of Defendant's data systems. In case of such a breach, Plaintiffs and the Class will not have a sufficient legal remedy because many of the resulting damages cannot be fully quantified, necessitating multiple lawsuits to address the same misconduct. While monetary damages are appropriate to compensate Plaintiffs and the Class for quantifiable and provable losses, they do not encompass the entirety of the injuries sustained, including damages that are not easily quantifiable or provable.

240. The hardship to Plaintiffs and the Class if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued.

241. Granting the requested injunction will not harm the public interest. On the contrary, it would serve the public by averting another data breach, thereby mitigating the injuries that would affect Plaintiffs, the Class, and the general public.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grants the following:

A. For an Order certifying the Class and Illinois Subclass, and appointing Plaintiffs and their Counsel to represent the Class and Illinois Subclass;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members;

C. For injunctive and other equitable relief as is necessary to protect

the interests of Plaintiffs and Class Members, including but not limited to an order that:

i. prohibits Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requires Defendant to protect all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requires Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiffs' and Class Members' respective lifetimes;

iv. requires Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. requires Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security

auditors;

vi. requires Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated; and,

vii. requires Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

Dated: February 6, 2024

Respectfully submitted,

TYCKO & ZAVAREEI LLP

By: */s/ Sabita J. Soneji*

Sabita J. Soneji
TYCKO & ZAVAREEI LLP
1970 Broadway, Suite 1070
Oakland, CA 94612
Telephone: (510) 254-6808
ssoneji@tzlegal.com

Counsel for Plaintiffs and Proposed Class